MATLAB Aerospace & Defense Technical Briefing

Modeling in the Stateflow® Environment to Support Launch Vehicle Verification Testing for Mission and Fault Management Algorithms in the NASA Space Launch System*

Luis Trevino, Ph.D.
Jacobs ESSSA Group – Marshall Space Flight Center
Mission & Fault Management (M&FM), EV43
Spacecraft and Vehicle Systems Department
04/27/2017
Huntsville, AL

** AIAA Paper previously presented at SPACE 2016, Long Beach CA*

AIAA Paper Co-Authors

- **Peter Berg**

  SLS State Flow Lead, M&FM Team
  Stinger Ghaffarian Technologies, Inc.
  Intelligent Systems Division
  NASA *Ames Research Center*

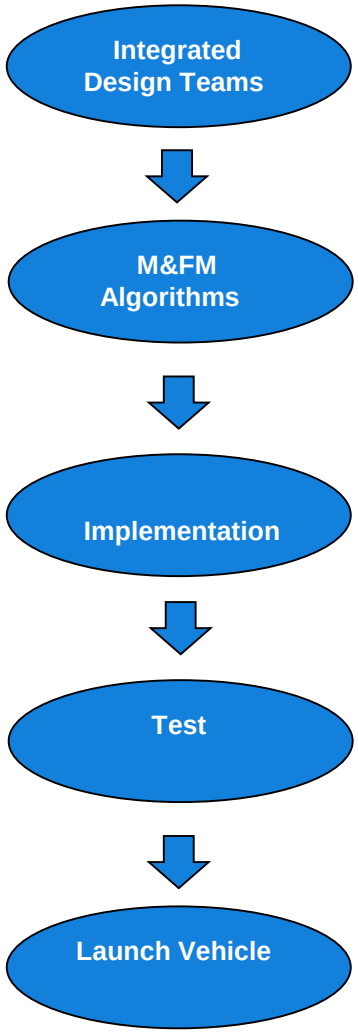
- **Dwight England**

  Chief, Integrated Systems Health Management & Automation Branch, EV43
  NASA *Marshall Space Flight Center*

- **Stephen B. Johnson, Ph.D.**

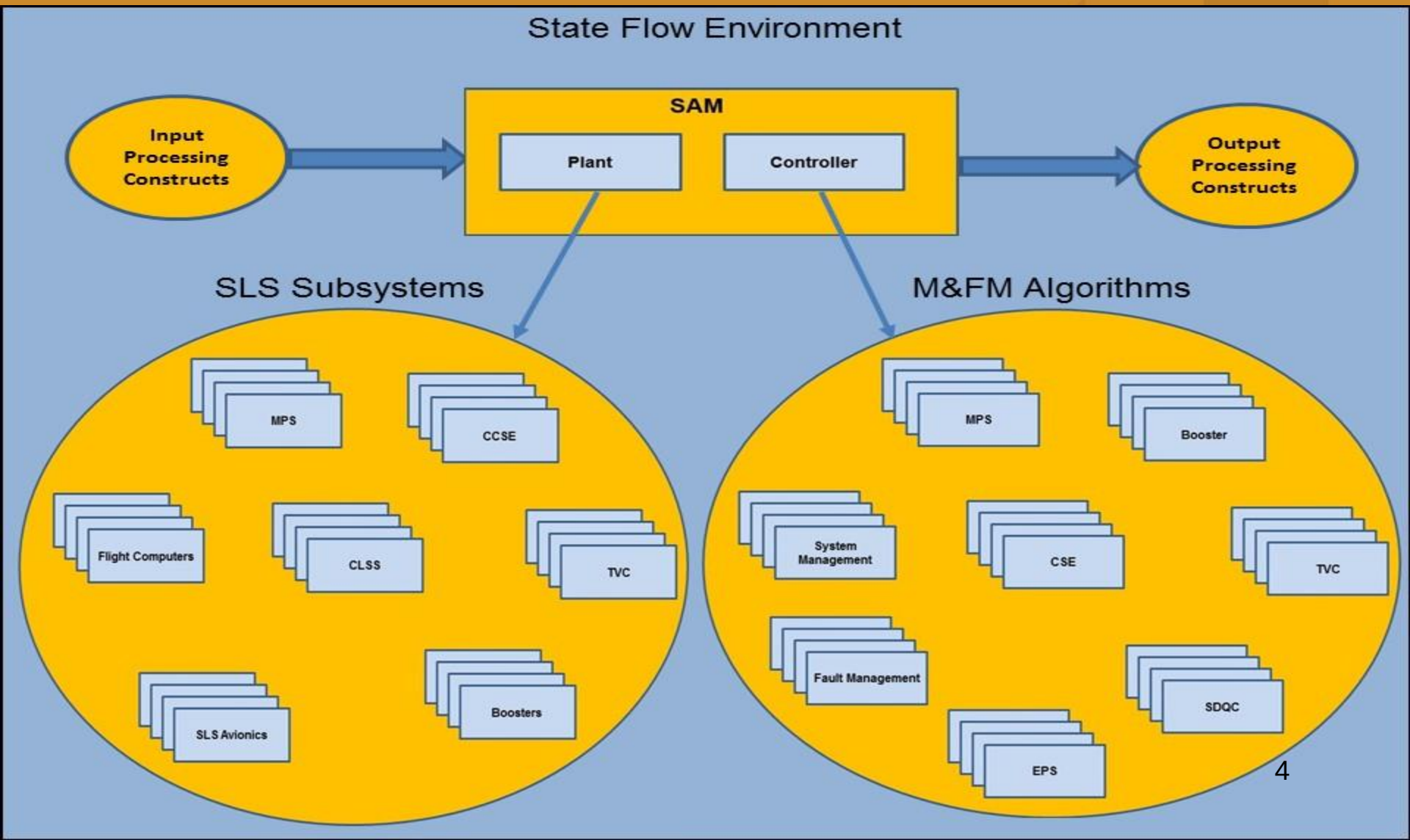
  Analysis Lead, M&FM Team
  Dependable System Technologies, LLC
  Jacobs ESSSA Group
  University of Colorado, Colorado Springs

Mission & Fault Management - SLS

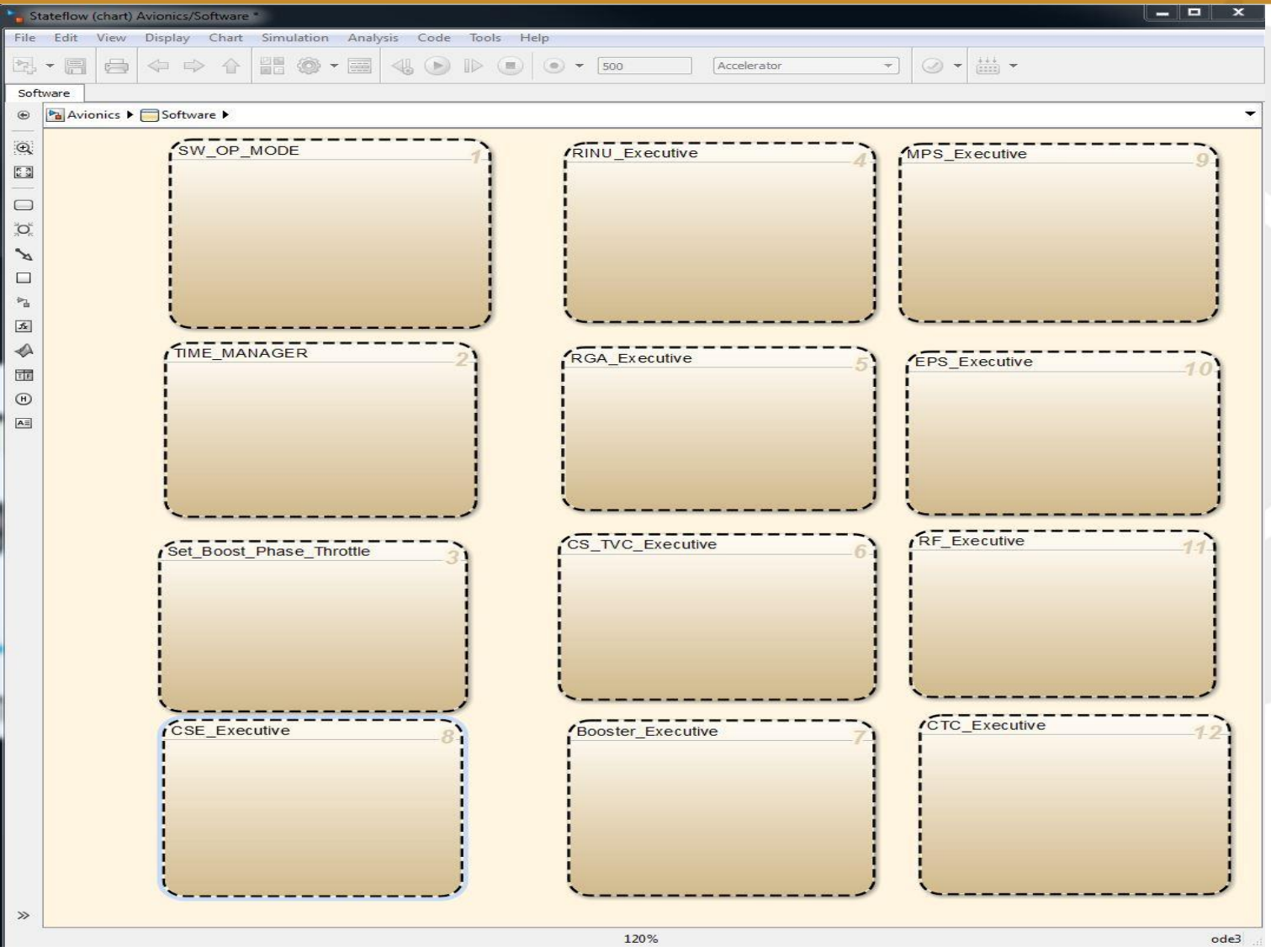


- Fault Management Software
  - Error Prone
  - Requirements and Design Phase
  - Other Factors
- Model Based Systems Engineering
  - Rich graphical constructs
  - Deterministic
  - Standards
- Previous NASA Stateflow® Applications
  - LADEE
  - Ares – Orion Command Abort
  - NESC – Toyota, Commercial Crew Program

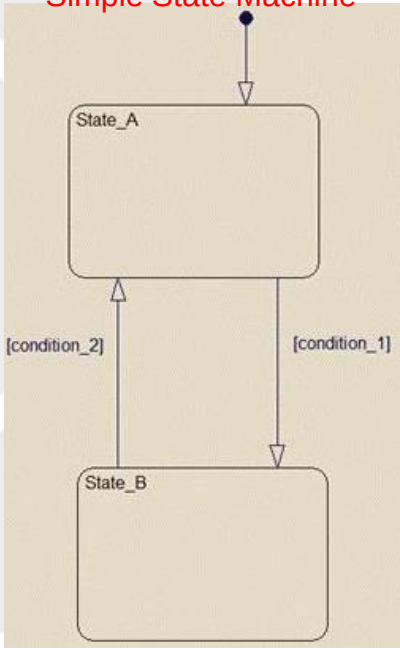
State Analysis Model (SAM)



MATLAB Stateflow

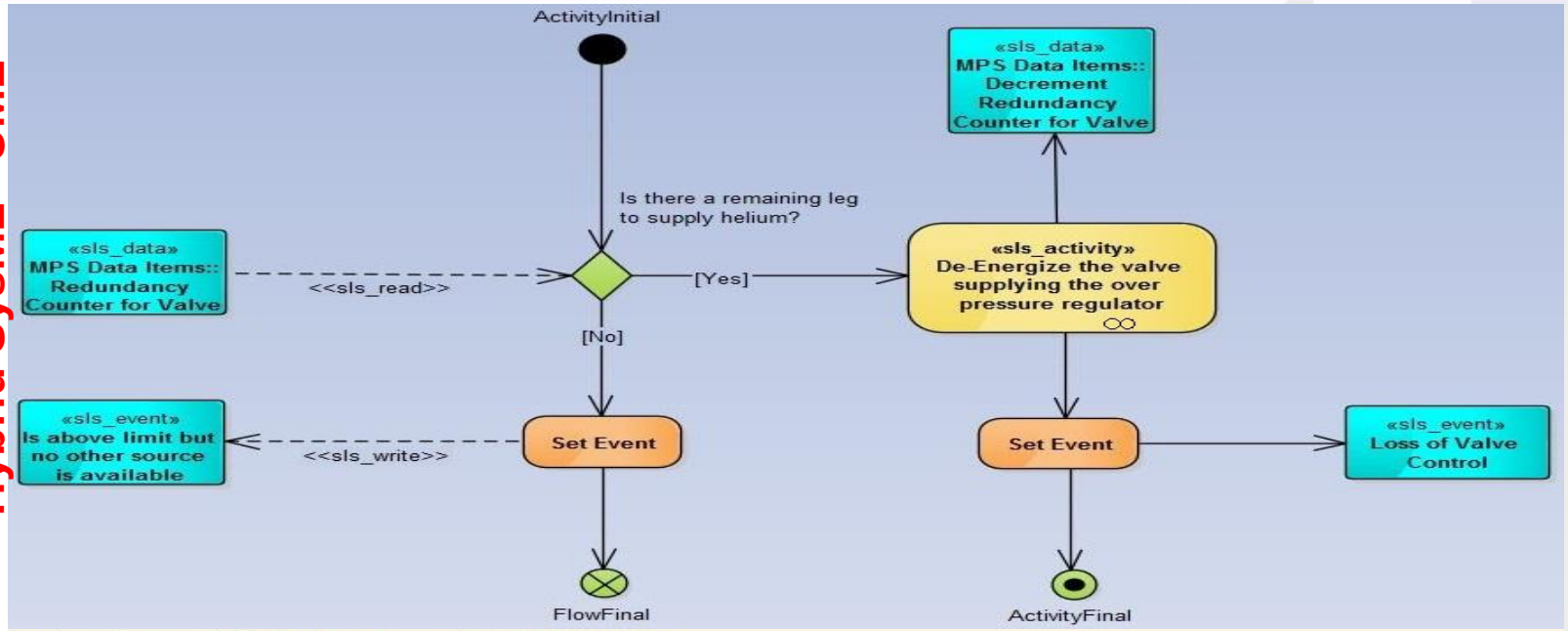


Simple State Machine

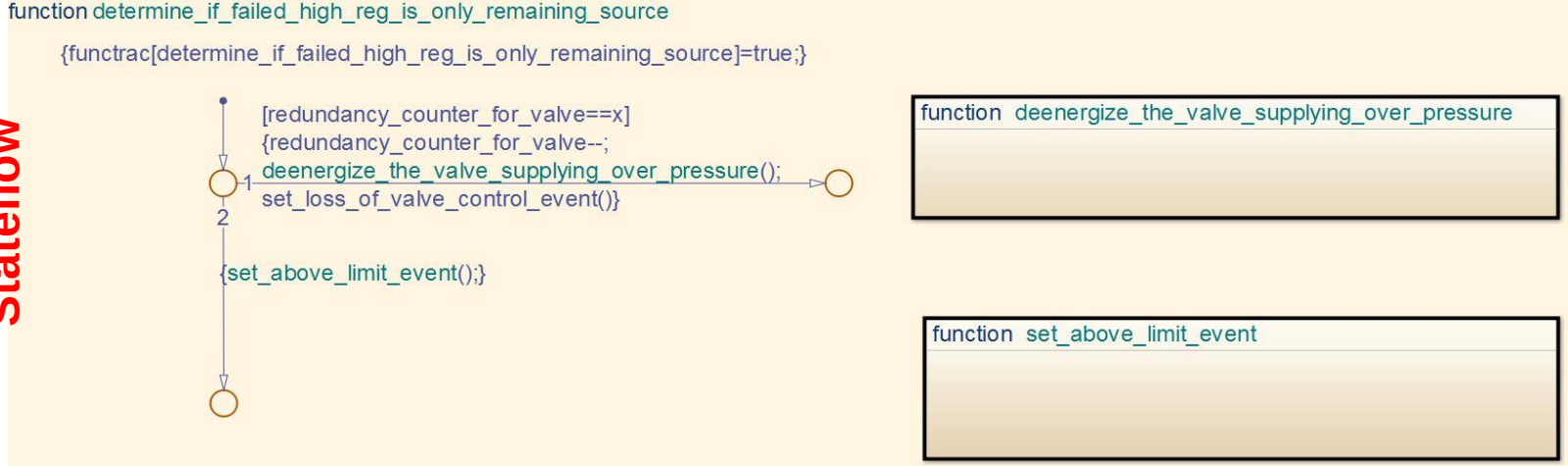


UML Modeling and Stateflow for M&FM

Hybrid SysML - UML



Stateflow



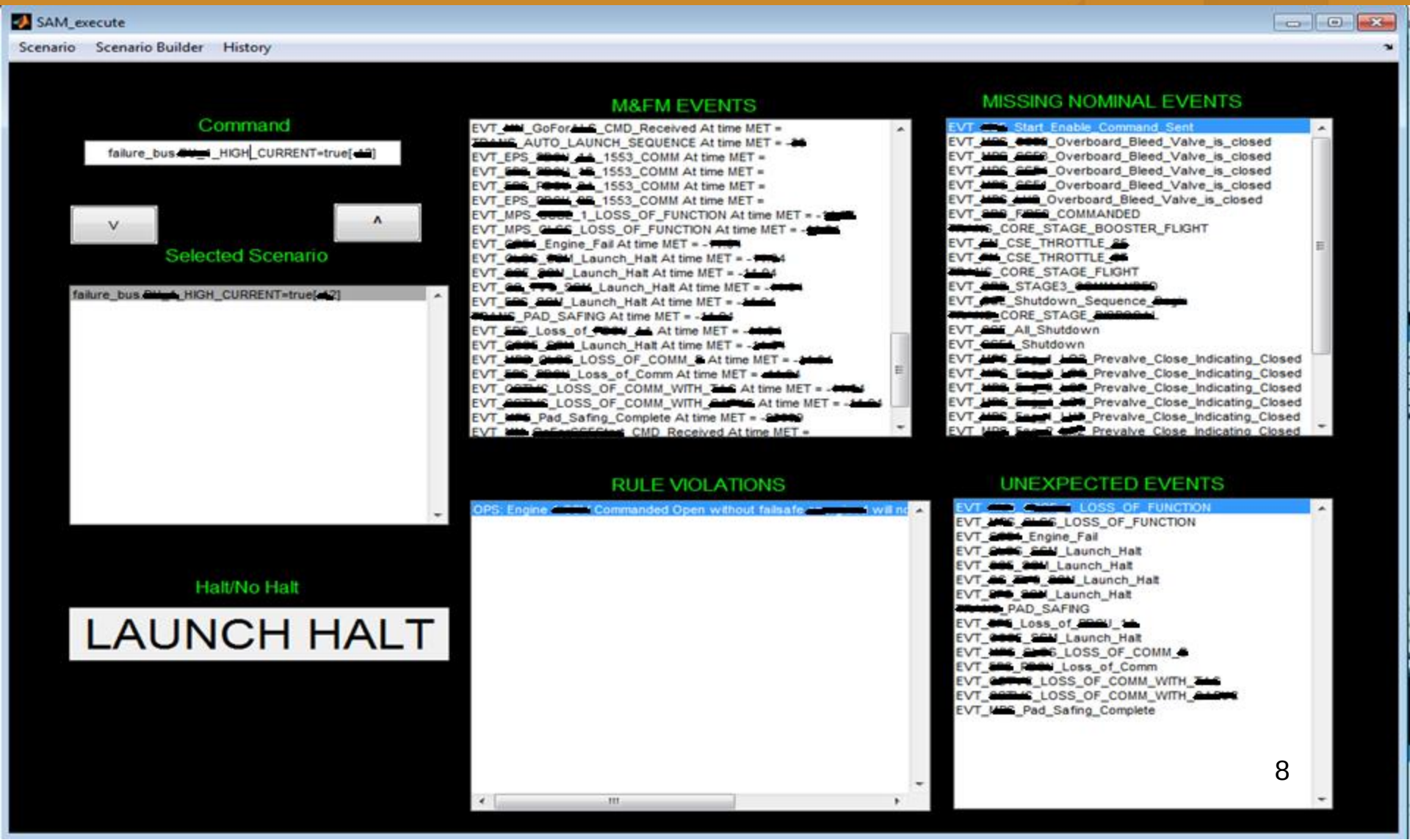
SAM Testing

- Script Driven → Ground Operations Timeline →
  Nominal Sequence Generator → Fault Generator
- Rule Checker → Analysis Report Generator →
  Timeline & State Report scripts → SAM Test Report

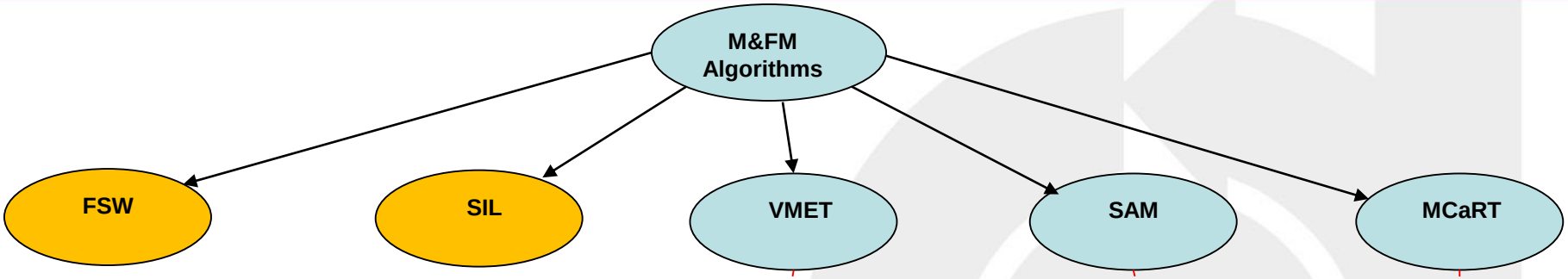
State Flow Env.

- User GUI
- Test Cases: Nominal, Off-Nominal, VMET, MCaRT, SIL
- TRAC Trouble Ticket System Summaries

User GUI


SAM_execute
Scenario
Scenario Builder
History
Command
failure_bus_HIGH_CURRENT=true
v
^
Selected Scenario
failure_bus_HIGH_CURRENT=true
Halt/No Halt
LAUNCH HALT
M&FM EVENTS
AUTO_LAUNCH_SEQUENCE At time MET =
1553_COMM At time MET =
1553_COMM At time MET =
1553_COMM At time MET =
1_LOSS_OF_FUNCTION At time MET =
LOSS_OF_FUNCTION At time MET =
Engine_Fail At time MET =
Launch_Halt At time MET =
Launch_Halt At time MET =
Launch_Halt At time MET =
PAD_SAFING At time MET =
Launch_Halt At time MET =
Loss_of_Comm At time MET =
Pad_Safing_Complete At time MET =
MISSING NOMINAL EVENTS
Start_Enable_Command_Sent
Overboard_Bleed_Valve_is_closed
Overboard_Bleed_Valve_is_closed
Overboard_Bleed_Valve_is_closed
Overboard_Bleed_Valve_is_closed
Overboard_Bleed_Valve_is_closed
COMMANDED
CORE_STAGE_BOOSTER_FLIGHT
CSE_THROTTLE_
CSE_THROTTLE_
CORE_STAGE_FLIGHT
STAGE3_
Shutdown_Sequence_
CORE_STAGE_
All_Shutdown
Shutdown
Prevalve_Close_Indicating_Closed
Prevalve_Close_Indicating_Closed
Prevalve_Close_Indicating_Closed
Prevalve_Close_Indicating_Closed
Prevalve_Close_Indicating_Closed
RULE VIOLATIONS
OPS: Engine Commanded Open without failsafe
UNEXPECTED EVENTS
LOSS_OF_FUNCTION
LOSS_OF_FUNCTION
Engine_Fail
Launch_Halt
Launch_Halt
Launch_Halt
Launch_Halt
PAD_SAFING
Launch_Halt
LOSS_OF_COMM_
Loss_of_Comm
LOSS_OF_COMM_WITH_
LOSS_OF_COMM_WITH_
Pad_Safing_Complete

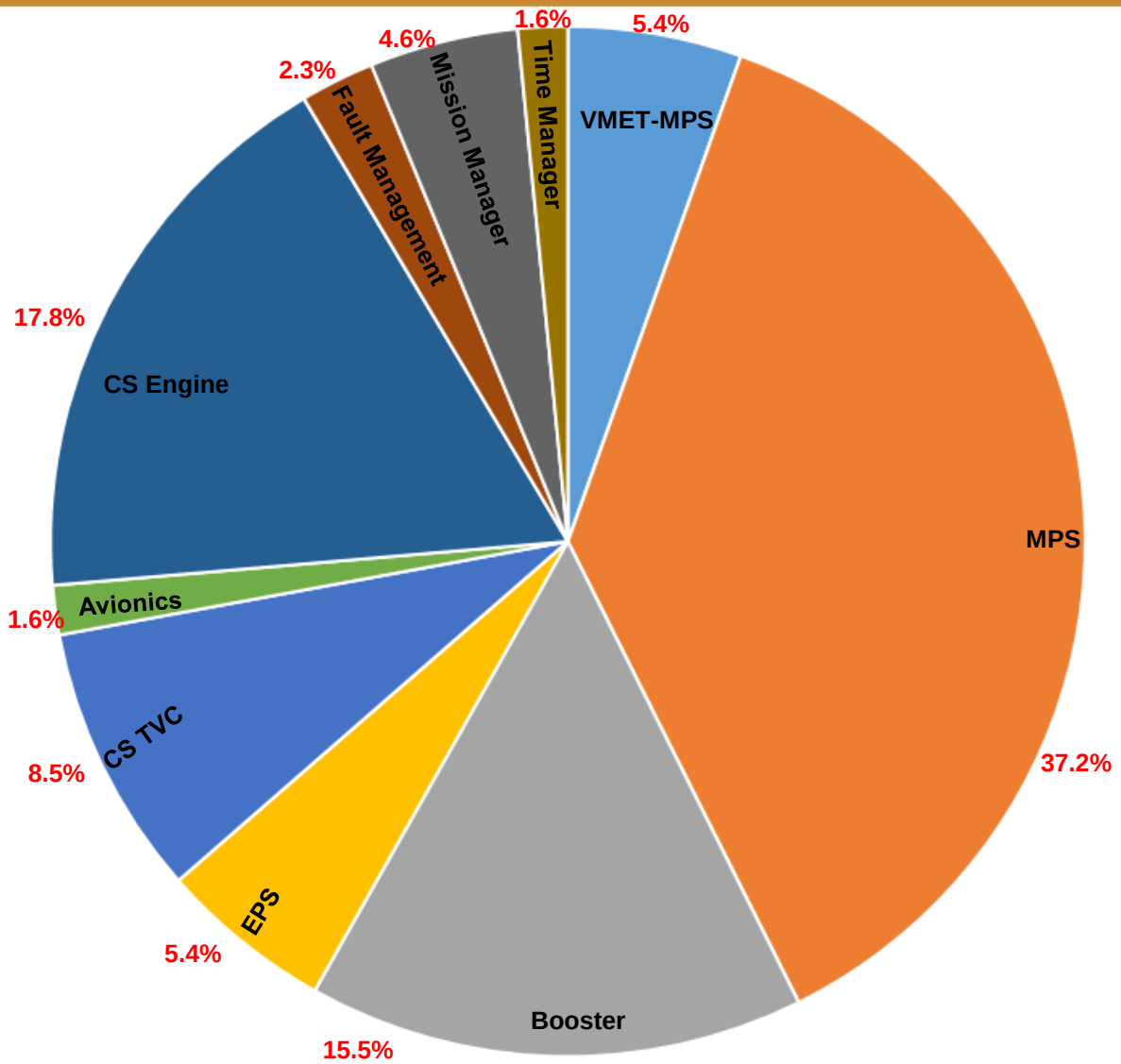
VMET, MCaRT, SIL Test Cases for the SAM



Test Case ID	Test Objective	Success Criteria	Duration / Fault Injection
MPS_Helium[redacted]	Test failure of helium isolation valve[redacted]	"EVT_[redacted]_HeliumValve[redacted]_Redundancy_Reduced" becomes "True" at Mission_Elapsed_Time = -[redacted] sec "EVT_[redacted]_Halt" becomes "True at Mission_Elapsed_Time = -[redacted] sec	Test duration is from Mission Elapsed Time = -[redacted] sec to -[redacted] sec Fault injected at Mission Elapsed Time = -[redacted] sec by setting Helium[redacted]_Energy = [redacted] & detected [redacted] cycles later at -[redacted] sec and [redacted] Halt set at Autonomous_Launch_Sequence at -[redacted] sec

Element	System	Response	Monitored Condition Name	Monitored Condition Description	Start Monitoring	Stop Monitoring	Units	Lower Trigger Limit (TBD)	Upper Trigger Limit (TBD)	Number of Indicators Needed to Generate Response
Booster	Igniter	Safing	Dual Boosters Ignition Failure	Both Boosters fail to ignite after T-[redacted] is reached	T+[redacted] msec	T+[redacted] msec	psia	[redacted]	[redacted]	2 of 2

Findings: VMET & SAM



MCaRT & SIL

19% of MCaRT entries tested
85.5% passed

45% of SIL test cases executed
27% passed

Finding Types

Logic Interpretation	30%
Editorials	55%
Logic Update	15%

SAM Forward Directions / Summaries

- Interactive Failures
- Prelaunch procedures → OMRs → LCCs → Rule Checker
- Hazardous State Identification
- Post Flight Analysis
- Other: EUS, crew habitat, payloads, proximity ops, rovers, robotic deep space missions, EDL ops
- MBE → M&FM Algorithms → FSW → Testing
- Challenges
- Questions